

Exhibit I



CHRISTIANATTAR

James W. Christian
jchristian@christianattarlaw.com

February 28, 2025

Via FedEx: 772400770336

Via Certified Mail Return Receipt: 9589 0710 5270 2796 8701 85

Via Regular Mail

Jennifer Vetrano
25 Pond Hollow Ln
West Creek, NJ. 08092

Re: Pre-Litigation Document Preservation Related to Potential Claims Involving Next Bridge Hydrocarbons, Inc.

**DEMAND FOR PRESERVATION OF ELECTRONICALLY
STORED INFORMATION**

To Whom it May Concern:

The undersigned has been retained as litigation counsel by Next Bridge Hydrocarbons, Inc. (hereinafter “Plaintiff” or “NBH”) to investigate and commence litigation against all parties who have engaged in a scheme of harassment, business disparagement, libel, slander, tortious interference, conspiracy, obstruction of justice and violations of the Administrative Procedures Act. We write to advise Jennifer Vetrano that litigation is being considered against certain individuals with respect to this matter. You may become a party or witness in this dispute and therefore, you have an obligation to preserve all documents and electronically stored information (“ESI,” as further defined below) that may relate in any way to the subject matter of this dispute (the “Claims”).

We hereby request that you, individually, or on behalf of any entities you control (“You”) preserve all documents, tangible things, and electronically stored information potentially relevant to the Claims such as documents, communications, and any other relevant materials including but not limited to:

1. All communications (emails, text messages, internal messaging systems, etc.) regarding NBH (including its board members, directors, officers, employees or agents) or Gregory McCabe
2. All Twitter (now X) data, including but not limited to:



www.christianattarlaw.com

1177 West Loop S, Ste 1700 | Houston, Texas 77027 | Phone: 713.659.7617 | Fax: 713.659.7644

Jennifer Vetrano
February 28, 2025
Page 2

- Direct messages (sent and received) related to NBH (including its board members, directors, officers, employees or agents) or Gregory McCabe
 - Public and private posts, tweets, replies, retweets, and quote tweets referencing NBH (including its board members, directors, officers, employees or agents) or Gregory McCabe
 - Account activity logs referencing NBH (including its board members, directors, officers, employees or agents) or Gregory McCabe
 - Any reports, complaints, or moderation actions related to content involving referencing NBH (including its board members, directors, officers, employees or agents) or Gregory McCabe
3. Any third-party communications (including correspondence with regulators or law enforcement) mentioning Plaintiff referencing NBH (including its board members, directors, officers, employees or agents) or Gregory McCabe
4. Metadata and logs associated with the above records, including timestamps, authorship, and any modifications

You should anticipate that files and much of the information relevant to Plaintiff's Claims are stored on your computers and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information ("ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, or optically stored on a computer, hard drive, cell phone, flash drive, CD, DVD or other electronic storage device as:

- Digital communications (e.g., e-mail, voice mail, text messaging, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., WAV and .MP3 files);
- Space Call Recordings;
- Webinars Recording;
- Podcasts Recordings;
- Video and Animation (e.g., AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;



www.christianattarlaw.com

1177 West Loop S, Ste 1700 | Houston, Texas 77027 | Phone: 713.659.7617 | Fax: 713.659.7641

Jennifer Vetrano
February 28, 2025
Page 3

- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO)

ESI resides not only in areas of electronic, magnetic, and optical storage media reasonably accessible to you, but also in areas that may not reasonably be accessible. You are obliged to preserve potentially relevant evidence from both these sources of ESI, even if it does not anticipate having to produce such ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary for Plaintiff to determine the nature and extent of any claims.

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information from January 1, 2018 to present.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents, files, and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and
- Executing drive or file defragmentation or compression programs.



Jennifer Vetrano
February 28, 2025
Page 4

Guard Against Deletion

You should anticipate that others may seek to hide, destroy, or alter ESI and act to prevent or guard against such actions. Especially where devices have been used for Internet access or personal communications, You should anticipate that users may seek to delete or destroy information they regard as personal, confidential, or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you. It is simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

Preservation by Imaging

You should take affirmative steps to prevent anyone with access to its data and archives from seeking to modify, destroy, or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space, and the swap file.

With respect to your hard drives and storage devices, the demand is made that you immediately obtain, authenticate, and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by you during the period from January 1, 2018 to present, as well as recording and preserving the system time and date of each such computer:

- Any Agents, Partners, or Collaborators of you concerning matters of NBH or its Officers, Directors, Shareholders, or Agents, including but not limited to Greg McCabe.

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

The term “computer” shall include any computer, hard drive, cell phone, flash drive, CD, DVD, or other devices capable of storing ESI.

Preservation in Native Form

You should anticipate that certain ESI, including but not limited to Word documents, spreadsheets, and databases, will be sought in the form or forms in which it is ordinarily



Jennifer Vetrano
February 28, 2025
Page 5

maintained. Accordingly, You should preserve ESI in such native forms, and it should not select methods to preserve ESI that remove or degrade the ability to search its ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino, G-mail) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downloaded or must be online 24/7. If you question whether the preservation method it pursues is one that we will accept as sufficient, please call us to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though we expect that You will act swiftly to preserve data on all devices, it should also determine if any home or portable systems may contain potentially relevant data. To the extent that you sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and your PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if you used online or browser-based e-mail accounts or services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.



Jennifer Vetrano
February 28, 2025
Page 6

Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like.

You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys and Third Parties

Your preservation obligation extends beyond ESI in its care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, You must notify any current or former representative, agent, attorney, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and it must take reasonable steps to secure its compliance.

System Sequestration or Forensically Sound Imaging

We suggest that, You, removing your ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step.

In the event You deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.



Jennifer Vetrano
February 28, 2025
Page 7

By “forensically sound,” we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called “unallocated clusters,” holding deleted files.

Preservation Protocols

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol if it will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol it intends to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If You do not currently have such expertise at its disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics.


Do Not Delay Preservation

I am available to discuss reasonable preservation steps; however, You should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which Plaintiff is entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Confirmation of Compliance

Please confirm as soon as practically possible and no later than March 14, 2025, that You have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If You have not undertaken the steps outlined above, or have taken other actions, please describe what it has done to preserve potentially relevant evidence.

Sincerely,



James Wes Christian